The Register-Guard
http://www.registerguard.com/

A Web world without borders

After 30 years of adding to our freedom of expression, the powers that be are plotting to take it all away

Published: *Midnight,* March 3

BY KATHERINE MAHER

For Foreign Policy Magazine

Nearly 365 years ago, more than 100 warring diplomats and princes got together in what is now northwestern Germany. There they signed a set of treaties that became the basic framework for our modern world: the Peace of Westphalia. Thanks to these dignitaries, we have territorial sovereignty: nation-states, demarcated by borders.

Westphalian sovereignty has become the basic ordering principle of our societies. Empires have risen and fallen, countries come and gone. The most successful states have established internal monopolies on information and resources and have exerted discretion on what trade, ideas, money or people crossed their borders.

But 30 years ago, humanity gave birth to one of the most disruptive forces of all time. On Jan. 1, 1983, the implementation of a standard protocol to allow computers to exchange data over a network turned discrete clusters of research stations into a distributed global phenomenon.

It took awhile for the Internet to make it from mainframes in universities to desktops in the home. But as it did, it birthed its own culture, full of shorthands and memes, communities and cesspools. This Internet was wild and woolly, unknown and unregulated. It was clearly a place, but a place without any familiar cultural signposts, a space beyond the boundaries of geography or identity. It deserved its own name: cyberspace.

Like all new frontiers, cyberspace’s early settlers declared themselves independent — most famously in 1996, in cyberlibertarian John Perry Barlow’s “A Declaration of the Independence of Cyberspace.” Barlow asserted a realm beyond borders or government, rejecting the systems we use to run the physical universe. “Governments of the Industrial World,” he reproached, “You have no sovereignty where we gather. ... Cyberspace does not lie within your borders.”

Barlow was right, in part. Independence was a structural fact of cyberspace, and free expression and communication were baked into the network. The standards and protocols on which the Internet runs are agnostic: They don’t care whether you are in Bangkok, Buenos Aires or Boise. If they run into an attempt to block traffic, they merely reroute along a seemingly infinite network of decentralized nodes, inspiring technologist John Gilmore’s maxim: “The Net interprets censorship as damage and routes around it.”

And unlike almost every other global resource in history, the Internet largely escaped government regulation at first . From the outset, it was managed not by governments but by a coalition of volunteer standards bodies and civil society groups awkwardly dubbed the multi-stakeholder system.

So lawmakers and politicians wrung their hands over the Internet’s lawlessness, gnashed their teeth at the moral decay of porn and downloads and despaired at their inability to legislate a place without a geography.

It was precisely this structural independence that transformed the Internet from a mere tool for information-sharing to an open forum.

The rise of self-publishing tools such as Blogger transformed cyberspace into a modern speaker’s corner, offering any motivated writer a soapbox. Initially, this online free expression was marginalized; the term “blogosphere” was originally a joke.

But bloggers kept plugging away. In liberal democracies, their free expression was guaranteed, and in closed societies connectivity often was too limited to draw any real attention.

In the past decade, however, all this has changed. Roughly 2 billion people use the Internet, in nearly every country in the world.

Blogs are now mainstream, and social networks have pushed self-publishing even closer to ordinary users, enabling instantaneous political and personal expression. And the Internet — this global resource, this wild space independent of states — has made its mark on our neatly ordered world of nations.

Information always has been power, and governments have long sought to control it. So for countries where information is tightly controlled by state television and radio stations, the Internet has been catastrophic. It gives people an outlet to publish what the media cannot, organize where organizing is forbidden, and revolt where protest is unknown.

And the Internet isn’t only threatening dictatorships. It has created new forms of political participation and protest in democracies, where it has been used to demand the decentralization of power to the people, facilitate radical transparency and information-sharing, demand responsive government, unseat corrupt authorities, organize marginalized minorities, and challenge the hegemony of traditional political heavyweights.

Naturally, systems of power have finally taken notice. Governments around the world have begun to assert control, seeking to carve up the global Internet, manage it within national borders, and impose Westphalian sovereignty on the wild World Wide Web.

It’s not entirely a new trend. The Great Firewall of China is almost as old as the Internet itself. But it is spreading, and taking new shapes.

Some of these efforts are explicitly about political control, imposing strict limits on what users within individual countries’ borders can access. Iran’s proposed halal Internet seeks to impose Islamic virtue on the browsing masses.

In Russia, the state agency Roskomnadzor enforces an Internet block list that has filtered the blogs of government critics. And in Pakistan, a recently revived proposal for a national firewall targets “blasphemy” as a proxy for ideas unpopular with the government.

Some of this, especially in the United States and Europe, is about commerce, reducing piracy and partitioning off intellectual property . But more tellingly, as countries seek to break up the Internet into neatly defined mirrors of themselves, they’re trying to redefine international norms in order to justify their actions.

At the summit of the International Telecommunication Union in Dubai this past December, a bloc made up of Russia, the United Arab Emirates, China, Algeria, Saudi Arabia and Sudan floated a proposal that tried to define a new term: the “national Internet segment,” or any telecommunications networks within the territory of a state. This language, later endorsed by Bahrain and Iraq, would have allowed countries full regulation of the Internet within their borders, from filtering content to imposing fees on foreign traffic. Ultimately, it was withdrawn.

But even without new international regulations, the technical backbone of our Internet is controlled increasingly at the national level. Two years ago, as the Arab world exploded in popular protest, governments responded simply by shutting off the Internet . Egypt’s mobile services were shut down and its Internet almost entirely disconnected, while in Libya, the Internet was throttled to a point of uselessness.

Recently, network research and analytics company Renesys tried to assess how hard it would be to take the world offline. They found that 61 countries are at severe risk for disconnection, with another 72 at significant risk.

That makes 133 countries where control is so centralized that the Internet could be turned off with not much more than a phone call. It seems our global Internet is not so global.

But as worrying as these threats are, at least they all have been civilian, rather than military, attempts to exert control over the web. That won’t be the case for long: Governments around the world are sounding alarms about the existential threat posed by cyberwar. From hostile foreign regimes to lawless nonstate actors, the threat of attacks on critical infrastructure to the theft of state secrets, the danger of economic warfare to corporate espionage, not a day goes by when cybersecurity is not in the news.

In response, governments around the world are devoting significant financial, military and personnel resources to developing frameworks for cybersecurity and cyberconflict.

Cyberspace is no longer the independent space of the cyberlibertarians; it is now a military domain. And when a freewheeling place such as the Internet militarizes, the Internet's laissez-faire culture of privacy, anonymity and free expression inevitably comes into conflict with military priorities of security and protocol.

In the United States, the Pentagon has been tasked with the development of rules of engagement for cyberconflict. On Feb. 12, President Obama issued a long-awaited executive order on cybersecurity and used his State of the Union address to call for new bipartisan legislation on the issue, emphasizing the need to protect critical U.S. infrastructure.

The very next day, Rep. Mike Rogers, R-Mich., and Rep. Dutch Ruppersberger, D-Md., reintroduced the Cyber Intelligence Sharing and Protection Act — a bill reviled by the privacy and civil liberties community for its lack of credible privacy protections and provisions for warrantless information-sharing.

Make no mistake: Cyberhostilities are on the increase, whether from petty cybercriminals or coordinated state efforts. From Stuxnet, which set back Iran's nuclear efforts, to Shamoon, which destroyed the control systems of oil giant Saudi Aramco, to the recent hacking of The Washington Post, The New York Times, Twitter and Facebook, we're seeing large-scale attempts to penetrate and interfere with both private and public systems.

While many cybersecurity experts disagree on how to best tackle the threats at hand, the most influential voices remain those arguing for greater militarization: investing in the development of strategic exploits or offensive capacity that double down on the idea of the Internet as a domain subject to dominance by state actors.

Nearly 365 years ago, those 100-plus princes and diplomats came together to end war — and in the process, created borders. The Internet broke those borders down, advancing the cause of fundamental rights, free expression and shared humanity in all its messy glory.

Now, to stifle political dissent and in the name of defending national security, governments are putting those borders back up — and in doing so, they're dragging the Internet into ancient history.
